PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-342276**

(43)Date of publication of application : **29.11.2002**

(51)Int.Cl. **G06F 15/00**
G06F 13/00
H04L 12/22

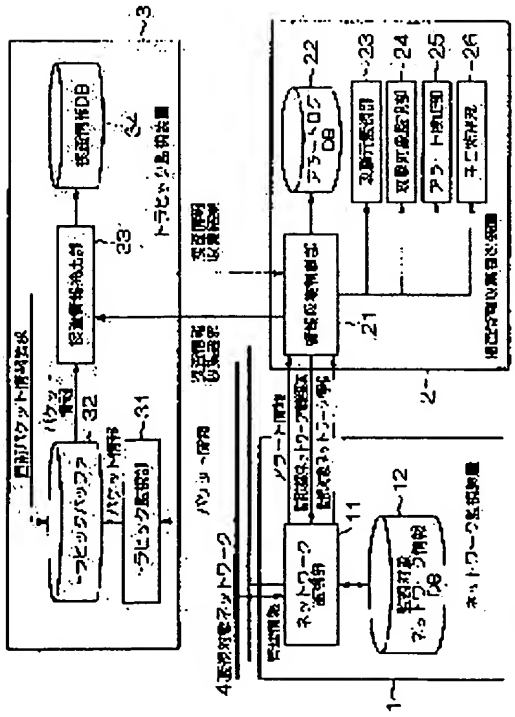
(21)Application number : **2001-148024**

(22)Date of filing : **17.05.2001**

(71)Applicant : **NTT DATA CORP**
CYBER SOLUTIONS INC

(72)Inventor : **KUWATA YOSHITAKA**
ITO YOSHIHIRO
KOBORI MAKOTO
KEENI GLENN MANSFIELD

(54) SYSTEM AND METHOD FOR DETECTING NETWORK INTRUSION



(57)Abstract:

PROBLEM TO BE SOLVED: To realize a high precision network type intrusion detecting device, and to protect the privacy of a normally accessing person by narrowing the targets of information collection down to suspects.

SOLUTION: A plurality of detection patterns corresponding to intrusion patterns are preliminarily prepared, and the detection patterns are switched dynamically as need by an investigation information collection controller 2. Also, a subtle omen indicating the possibility of intrusion is defined as an object to be monitored by the investigation information collection controller 2, and a network monitoring device 1 and a traffic monitoring device 3 are controlled, so that the monitorial system can be changed according to the level. Moreover, a fixed amount of packets are always held by the traffic monitoring device 3, so that the previous state can be utilized as

* NOTICES *

CLAIMS

[Claim(s)]

[Claim 1]A network intrusion detection system comprising:

A network monitor which acquires network management information from a surveillance object network, and detects existence and its invasion pattern of network invasion.

A search information gathering control device which collects investigative information which changes dynamically a detection pattern applicable by performing collation with said invasion pattern and two or more detection patterns beforehand prepared according to each of said invasion pattern, and follows the detection pattern concerned.

[Claim 2]The network intrusion detection system according to claim 1 having a traffic monitoring instrument which outputs investigative information according to said detection pattern also including information in front of invasion according to a demand from said search information gathering control device.

[Claim 3]The network intrusion detection system according to claim 1, wherein said investigative information collection control device is provided with the attacking agency Monitoring Department which does the intensive surveillance of the communication by a specific invader detected by said network monitor.

[Claim 4]The network intrusion detection system according to claim 1, wherein said investigative information collection control device is provided with the target-of-attack Monitoring Department which does the intensive surveillance of the communication to a specific target of attack detected by said network monitor.

[Claim 5]The network intrusion detection system according to claim 1 provided with an alert verification part which verifies whether said investigative information collection control device has the detection information that it is otherwise the same, to detection information detected by said network monitor.

[Claim 6]Said alert verification part refers to a database with which surveillance object network information

claim 6 characterized by comprising the following.

A means pattern in which the means sequence and means confrontation processing were defined beforehand as for said investigative information collection control device.

The means Monitoring Department which performs means confrontation processing which includes a shutout of the target when a means candidate is scolded and the means candidate concerned is found by comparing investigative information from an invading agency host acquired from said traffic monitoring instrument.

[Claim 8]Acquire network management information from a surveillance object network, and existence and its invasion pattern of network invasion are detected, A network invasion detection method collecting investigative information which changes dynamically a detection pattern applicable by performing collation with said invasion pattern and two or more detection patterns beforehand prepared according to each of said invasion pattern, and follows the detection pattern concerned.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]this invention -- a network intrusion detection system and a method for the same -- in detail, By improvement of the network type trespass detecting device (NIDS:NetworkIntrusion Detection System) which detects the existence of network invasion, and cooperation with a managerial system. It is related with a synthetic security system which acquires the information before and behind a security incident in detail, and a method for the same.

[0002]

[Description of the Prior Art]The service provision to corporate transactions and the customer who utilized the Internet is a problem of the utmost importance for the company which gropes for strategic business deployment. However, the communication environment of the Internet is exposed to various threats of the unauthorized entry and virus infection by a hacker. By the way, it connects with the network in a company in the middle of the Internet, and a fire wall functions as a sensor which intercepts unjust access from the Internet. In the network system which installed the fire wall, gateway access to the exterior from an inside is enabled, and the various services of the Internet can be safely used now. However, in the unauthorized entry by a hacker, there is a danger of receiving various attacks, such as an attack which poked the security hole of the fire wall main part, an attack by port scan, and a use impossible attack which blocks access.

[0003]

[Problem(s) to be Solved by the Invention]As described above, while the illegal use of a computer system

system using the conventional NIDS, it has a fault of (1) – (5) enumerated below.

[0004](1) Only detection according to the detecting pattern defined uniquely beforehand can be performed, therefore there is much erroneous detection.

(2) With the advancement of an invasion means, the detection definition pattern becomes complicated and description of a definition is difficult.

(3) Since only the packet defined as NIDS being inaccurate was detected, information required in order to supervise a series of the actions of the aggressor before and behind unjust detection was not able to be acquired. In order to record a "means" which comprises plural steps, means only have operating packet monitoring and a recorder independent of NIDS after detecting injustice at NIDS, and promptly detailed information was not able to be acquired. When the dynamic surveillance system according to a threatening grade could not be built but it was always considered as the wax in the detailed information about invasion, while many computer resources were required for packet monitoring and recorders, such as a disk and CPU, the analysis of the huge collected information was impossible as a matter of fact.

(4) When invasion was detected, it was difficult to be invasion with the strange result, or to verify whether it is erroneous detection. It needed to be made setting out which acquires detailed information beforehand in order to verify a detection result, and even if it changed so that after-detection detailed information might be acquired, in many cases, since invasion had already finished, it had become too late.

(5) There was a possibility of infringing on a regular access person's privacy for information gathering.

[0005]In light of the above-mentioned circumstances, this invention is a thing.

the purpose preparing two or more detecting patterns which were alike and responded, and it changing this dynamically and it if needed, It is providing a network intrusion detection system which achieved highly precise-ization of NIDS, and a method for the same by increasing sources of information by preparing the structure which acquires the detailed information, and utilizing as investigative information, and cooperating with a traffic monitoring instrument, and the detailed information coming to hand.

By also making minor signs as show the possibility of invasion into a surveillance object, and making a network surveillance system change according to the level, The collection object of information is narrowed down to a suspicious person, and also let it be the purpose to provide a network intrusion detection system which protects a regular access person's privacy, and a method for the same.

[0006]

[Means for Solving the Problem]This invention is characterized by comprising the following, in order to solve the above-mentioned technical problem.

A network monitor which acquires network management information from a surveillance object network, and detects existence and its invasion pattern of network invasion.

A search information gathering control device which collects investigative information which changes dynamically a detection pattern applicable by performing collation with said invasion pattern and two or more detection patterns beforehand prepared according to each of said invasion pattern, and follows the

from said search information gathering control device.

[0008]In this invention, said investigative information collection control device was provided with the attacking agency Monitoring Department which does the intensive surveillance of the communication by a specific invader detected by said network monitor.

[0009]In this invention, said investigative information collection control device was provided with the target-of-attack Monitoring Department which does the intensive surveillance of the communication to a specific target of attack detected by said network monitor.

[0010]In this invention, it had an alert verification part which verifies whether said investigative information collection control device has the detection information that it is otherwise the same, to detection information detected by said network monitor.

[0011]In this invention, said alert verification part, At least one of alert object hosts' importance, alert object hosts' traffic volume, and the importance of alert object service is made to reflect in an information acquisition level of investigative information from said traffic monitoring instrument with reference to a database with which surveillance object network information was stored.

[0012]In this invention, said investigative information collection control device, A means candidate is scolded by comparing a means pattern in which the means sequence and means confrontation processing were defined beforehand with investigative information from an invading agency host acquired from said traffic monitoring instrument, When the means candidate concerned was found, it had the means Monitoring Department which performs means confrontation processing including a shutout of the target.

[0013]By preparing two or more detecting patterns which responded to an invasion pattern beforehand in the above-mentioned composition, and preparing structure changed dynamically if needed, From most important method according information made into an object of collection to the existing NIDS, by extending to extensive information including network management information, sources of information can be increased and it can utilize as investigative information. Highly precise-ization of NIDS can be attained by performing fine control of a detecting pattern of NIDS and an information acquisition pattern. An investigative information collection control device is utilizable as detection information also including the last state by always holding a constant rate of packets with a traffic monitoring instrument. Therefore, verification of a means after an invasion inspection from this packet currently held and information acquired by the above and invasion is attained. Minor signs as show the possibility of invasion can also be made into a surveillance object, and a surveillance system can be made to change with an investigative information collection control device according to the level. Specifically a traffic monitoring instrument pair will be carried out if needed, directions will be issued, the information acquisition level will be changed dynamically, as a result, a collection object of information will be narrowed down to a suspicious person, and a regular access person's privacy can be protected.

[0014]In order to solve the above-mentioned technical problem, this invention acquires network management information from a surveillance object network. Detect existence and its invasion pattern of

including information in front of invasion.

[0016]

[Embodiment of the Invention]Drawing 1 is a block diagram showing one embodiment of the network intrusion detection system in this invention. The network intrusion detection system of this invention comprises the network monitor 1, the investigative information collection control device 2, the traffic monitoring instrument 3, and the surveillance object network 4. The network monitor 1 acquires network management information from the surveillance object network 4, and has a function which detects the existence and its invasion pattern of network invasion. The investigative information collecting apparatus 2 changes dynamically a detection pattern applicable by performing collation with an invasion pattern and two or more detection patterns beforehand prepared according to each of an invasion pattern, and has the function to collect the investigative information according to the detection pattern concerned. The traffic monitoring instrument 3 has a function which outputs the investigative information according to a detection pattern also including the information in front of invasion according to the demand from the search information gathering control device 2.

[0017]The network monitor 1 comprises the network Monitoring Department 11 and surveillance object network information DB(database)12. The network Monitoring Department 11 acquires network management information from the surveillance object network 4, By detecting an unauthorized entry, detection information (alert information) is given to the investigative information collection control device 2, and the surveillance object network information accumulated in surveillance object network information DB12 based on the surveillance object network information demand from the investigative information collection control device 2 is provided. The IP packet information which comprises a header and a pay load (contents) is accumulated in surveillance object network DB12 besides network configuration information, servicing information, and operation information. As network configuration information, the detailed routing information of apparatus, such as a host, a router, etc. which were connected to the network, as servicing information, As operation information, the traffic information for every host and the traffic information (access frequency) for every service are accumulated for a host's service provision policy and the service actually provided for a host. The information about a host and the importance of service, and the height of traffic volume is also included in surveillance object network DB12, and the example is shown in drawing 6 and drawing 7. Here, although surveillance object network information DB12 explains as a thing in the network monitor 1, it may be in the investigative information collection control device 2 mentioned later. In this case, since all fundamental control sections are brought together in the investigative information collecting apparatus 2, it is possible to make simple the composition and the function of the network monitor 1.

[0018]The investigative information collection control device 2 is constituted from alert log DB(database)22, the attacking agency Monitoring Department 23, the target-of-attack Monitoring Department 24, the alert verification part 25, and the means Monitoring Department 26 by the core in the information gathering

instrument 3 is started and it is shown in drawing 2, It comprises the rule analyzing parts 211, the pattern match part 212, the action execution part 213, and the rule library 214.

[0019]It is as having described above that two or more detection patterns are beforehand prepared for the investigative information collecting apparatus 2 according to each of an invasion pattern. The detection pattern is library-ized as a rule here, and it memorizes all over the rule library 214. The rule analyzing parts 211 analyze by reading this rule, compare with the IP packet obtained via the network Monitoring Department 1 in the pattern match part 212, and perform action according to the detection pattern which coincidence was able to take by the action execution part 213. Actions here are the recording start of traffic, a stop, specific attack former surveillance, the surveillance for specific, alert verification, and means surveillance, and a rule set is changed if needed.

[0020]An example of a rule form and a rule is shown in drawing 3 and drawing 4, respectively. A rule is defined by the "pattern" part and "action" part as shown in drawing 3 (a). As a pattern, tcp (transfer control protocol), The protocols (protocol), such as udp (userdatagram protocol), DESUTE nation specifications (dest-spec), such as sauce specifications (source-spec), such as an IP address and a port number, both directions/uni directional (<>|->), an IP address, and a port number, the other matching specifications (matchinf-spec) of a payload part, etc. are described. * seal in a figure means a repetition.

[0021]Drawing 3 (b) expresses the form of a pattern part, and it besides the above-mentioned IP address and a port number, A title value (ttl), an ICMP (Internet Control Message Protocol) type (itype), The ICMP code (icode), the minimum FUARAGUMENTO payload size (minfrag), There are the contents (content) of a TCP sequence number (seq), a TCP-ACK (Acknowledge) number (ack), the fragmentation ID number (id) of an IP header, payload size (dsize), and the packet for pattern matches. The alert (alert) which drawing 3 (c) expresses action information and sends alert information to the manager (information gathering control section 21) of an upper device, There are log (log) which stores a message in a log file, a fork rule set (fork-ruleset) which changes a rule set, the record (record) which performs control of the traffic monitoring instrument 3, etc.

[0022]Drawing 4 shows each example of a rule in the case of performing attacking agency surveillance, when performing attacking agency surveillance according to the form shown in drawing 3, and performing target-of-attack surveillance, and port scan is detected. In rule name "sniffing-host" by attacking agency surveillance, Mean what the arbitrary port of IP address"192.168.10.10" is supervised with an arbitrary protocol, and all are recorded on the arbitrary port of variable $HOME_NET for, and in target-of-attack surveillance. In rule name "watch-home", it means supervising an arbitrary protocol, an arbitrary IP address, and an arbitrary port, and recording 20 bytes of pay-load head on the arbitrary port of IP address"192.168.0.5" in addition to all the header information. In [when port scan is detected and it performs attacking agency surveillance] rule name "switch-snif", It means changing a rule set to "snifing-host" which supervises the arbitrary port of an arbitrary IP address with an arbitrary protocol, and is in variable $source address after arbitrary port scan detection of variable $HOME_NET

monitor 1. The alert verification part 25 has the function to verify whether there is any detection information that it is otherwise the same, to the detection information detected by the network monitor 1. The means Monitoring Department 26 refers to surveillance object network information DB12, Make at least one of alert object hosts' importance, alert object hosts' traffic volume, and the importance of alert object service reflect in the information acquisition level of the investigative information from the traffic monitoring instrument 2, and. A means candidate is scolded by comparing the investigative information which shows the history from an invading agency host acquired from the means pattern in which the means sequence and means confrontation processing were defined beforehand, and the traffic monitoring instrument 2, When the means candidate concerned is found, it has the function to perform means confrontation processing including the shutout of the target. The individual case about the attacking agency Monitoring Department 23 and the target-of-attack Monitoring Department 24 is as having been shown in drawing 4, and the details about the alert verification part 25 and the means Monitoring Department 26 are later mentioned using an individual case.

[0024]The traffic monitoring instrument 3 comprises the traffic Monitoring Department 31, the traffic buffer 32, the investigative information extraction part 33, and investigative information DB(database)34. The traffic Monitoring Department 31 has a function which always accumulates a constant rate of packets obtained from the surveillance object network 4 in the traffic buffer 32. The traffic buffer 32 is a buffer of a FIFO (First-In First-Out) method, and transmits the already accumulated packet information the whole predetermined unit based on the packet information requirements from the investigative information extraction part 33. The investigative information extraction part 33 accumulates the transmitted packet information in investigative information DB34, and it also has a function which supplies the detailed information according to the demanded information acquisition level by searching investigative information DB34 based on the investigative information collection request emitted from the investigative information collection control device 2.

[0025]Drawing 5 is a key map of operation illustrating and showing a network security system about operation of the investigative information collection control device 2 shown in drawing 1. Here, the intrusion detection information and pertinent information over the server 5-1 on the surveillance network 4-1 are detected with the network monitor 1-1, and it notifies to the investigative information collection control device 2 (**). In order to strengthen the surveillance of the link of relation, the investigative information collection control device 2 emits directions so that it may supervise intensively on the basis of the source address information etc. which carried out the grouping of the network monitor 1-2 and the network monitor 1-3, and were detected with the network monitor 1-1 (**). By the network monitor 1-2 and 1-3, the information about a "means" is collected simultaneously (**). In order to realize looking out for the attack on the network 4-2 which is different in the surveillance network 4-1 a priori, it supervises whether the means which became clear by ** also to the network monitor 1-4 which is directly unrelated is used, and it is striving for early watch (**)

object-hosts information from surveillance object network information DB12 first on the assumption that object OS, an object network service, an object version, an object patch level, etc. are set up (Step S61). The alert verification part 25 confirms whether OS for an alert is equal to target-of-attack OS (Step S62), When judged with it not being equal, it is confirmed whether in invalid alert processing, (Step S63) and when it is judged with it being equal, the network service for an alert is still more nearly working at a target-of-attack host (Step S64).

[0027]When it judges that the network service for an alert is not working by an attack host, here, In network service verification processing (Step S65), when judged with it being working, it is confirmed whether the version of the network service for an alert is still the same as that of a target-of-attack host (Step S66). The network service for an alert judges whether it is working at present by a target-of-attack host by what network service verification processing is performed for (Step S65) (Step S610), In not being working, it performs invalid alert processing at Step S612, and when working, unjust service processing is performed at Step S611. When it judges that the version of the network service for an alert differs from a working thing by a target-of-attack host, the effective alert processing which shows drawing 7 invalid alert processing (Step S67) when judged with it being equal is started (Step S68). And the alert verification processing from Step S61 described above until all the target-of-attack hosts ended to S68 is repeated (Step S69).

[0028]In the flow chart shown in drawing 7, the alert verification part 25, Alert object hosts' importance defined as surveillance object network information DB12 is checked, and when judged with importance being high as compared with the threshold set up beforehand, processing which updates the importance +one time is performed (Step S72). When importance is not so high, with reference to surveillance object network information DB12, alert object-hosts traffic volume is checked further, and when judged with it being high, the importance of traffic volume as well as previous importance is updated +one time. When traffic volume is not so high, the importance of alert object service is checked further, and when importance is high, the importance is updated +one time. When importance is not so high, effective alert processing is ended. The reason the alert verification part 25 controls importance other than mere alert verification processing here is for using it for level judgment when controlling the traffic monitoring instrument 3 and collecting detailed information.

[0029]The example of input and output for alert verification is shown in drawing 8. In drawing 8, the alert verification part 25 receives alert information as input via the information gathering control section 21 first from the network Monitoring Department 1. In ID, the address of "1080" and alert object hosts input "192.168.0.1", In a kind, "SNMP public access" and a network service name "SNMP:Simple Network Management Protocol", a port number — " — 161 — " — a version — arbitrary — a version — from — changing — an alert — information — # — one — ID — " — 1080 — ". In alert object hosts' address, "192.168.0.1" and a kind "anonymous ftp", A network service name is "FTP:File Transfer Protocol", and port numbers are "21" and alert information #2 to which a version changes from an arbitrary version. On the other hand, to target-of-attack network information DB260, In a host, "192.168.01" and a network service

processing will be performed [1 / alert information #] for effective alert processing as an output item here as a result of verification.

[0030]Drawing 9 and drawing 10 show the example of the means surveillance by the means Monitoring Department 26, are a flow chart about the flow of processing, and describe the example of a means pattern according to list form, respectively. As shown in drawing 10, four kinds of means patterns shown by (1) to (4) are illustrated, and a means sequence and means confrontation processing are shown in each here. Namely, as confrontation processing of three means sequences in which there is port scan and buffer overflow is detected by the attack on Webb CGI in a means pattern (1), An attack former host's (source) shutdown and the alert of the purport "it was invaded into the target host with sauce" are emitted. As confrontation processing of four sequences in which there is port scan and buffer overflow was detected after "finger" and "telnet" service in the means pattern (2), The shutout of the partner point (source) and the alert of the purport "it was invaded into the target host with sauce" are emitted.

[0031]On the other hand, a means pattern (3) shows the case where an attack means from two or more hosts is detected, Two or more distributed DOS attacks from a host (Other_Hosts) to object hosts (target) are detected, When the Ping_Of_Death attack to object hosts from a partner point host (Source) is detected succeedingly, a shutout of a partner point host and two or more hosts and the alert of the purport "it was invaded into the target host by the sauce host" are emitted as the countermeasures. A means pattern (4) detects the branching DOS attack to the object hosts (DNS_SERVER) who perform DNS from two or more hosts (Other_Hosts), When the message corresponding to DNS from a host which is not simultaneously registered as DNS (Domain Name Server) is checked, a shutout of a partner point host and two or more hosts and the alert of the purport "the DNS server was downed" are emitted.

[0032]In the flow chart shown in drawing 9, the means Monitoring Department 26 acquires a means pattern from means pattern DB270 after receiving alert information (Step S91). As a means pattern, as shown in drawing 10, a confrontation sequence and its confrontation processing are described. The means Monitoring Department 26 acquires the hysteresis information from an attacking agency host (source) by referring to investigative information DB34 again (Step S92). And in the case of a means from two or more hosts, further in addition to this, the means Monitoring Department 26 acquires the hysteresis information from a host (Step S93), and performs collation of a means pattern and a history (Step S94). Here, when in agreement, a means candidate is scolded (Step S95), when inharmonious, it returns to processing of Step S91, and the following means pattern information is acquired, and henceforth, the above-mentioned operation is repeated until a means pattern continues (Step S96). And when a means candidate is scolded, processing described by (Step S97) means pattern DB270 as means confrontation is performed. Namely, an attacking agency host's (source) shutout and the alert of the purport "it was invaded into the target host with sauce" are emitted so that it may be described by drawing 10, When an attack means from two or more hosts is detected, a shutout of other hosts containing the partner point and the alert of the purport "the DNS server was downed" are emitted, for example.

according the information made into the object of collection to the existing NIDS, by extending to extensive information including network management information, sources of information can be increased and it can utilize as investigative information. Highly precise-ization of NIDS can be attained by performing fine control of the detecting pattern of NIDS and an information acquisition pattern. If the port scan to all the ports is detected and disquieting access for example, to a smtp port is specifically detected from the same host after that, the rule of NIDS will be changed so that the invasion check pattern about the brittleness of smtp may be applied preponderantly.

[0034]Minor signs as show the possibility of invasion are also made into a surveillance object, and a surveillance system is made to change with the investigative information collection control device 2 according to the level. Specifically it will receive traffic monitoring instrument 3 if needed, directions will be issued, the information acquisition level will be changed dynamically, as a result, the collection object of information will be narrowed down to a suspicious person, and a regular access person's privacy can be protected. For example, at a certain step, when the disquieting motion turned to the invasion from a certain IP address by NIDS is detected, a part for n bit is recorded from a head to all the packets to the particular port which exists from the IP address. And when the disquieting motion from the ID address continued and it is detected n minutes or more at the following step, A part for n bit is recorded from the head of all the packets to all the ports from the ID address, and also when the invasion possibility from the ID address is detected at the following step, all the packets of the ID address are recorded.

[0035]The investigative information collection control device 2 can utilize the last state as an examination report by always holding a constant rate of packets with the traffic monitoring instrument 3. Verification of a means after the invasion inspection from this packet currently held and the information acquired by the above and invasion is attained. For example, although the trace which tried invasion by "smtp" to IP address "port from all the records of communication content from 10.2.190.38"" 25" was found, The place which it became clear that invasion was finished with failure, and investigated communication recording [/ in addition to port "25" of the point], It becomes clear that the communication by the format over "cgi" of port"80" do not get it used to seeing tried the strange invasion method for "cgi" of port"80" as a result when many things became clear after a previous example.

[0036]The above-mentioned network monitor 1 and the investigative information collection control device 2, The traffic monitoring instrument 3, the network Monitoring Department 11, and the information gathering control section 21, The attacking agency Monitoring Department 23, the target-of-attack Monitoring Department 24, and the alert verification part 25, The means Monitoring Department 26, the traffic Monitoring Department 31, and the operation information extraction part 33, The procedure performed by each of the rule analyzing parts 211, the pattern match part 212, and the action execution part 213 is recorded on the recording medium in which computer reading is possible, The program recorded on this recording medium may be made to read into a computer system, and the function in each device mentioned above by performing may be performed. HARDWARE such as OS and peripheral equipment shall be included

magneto-optical disc, ROM, and CD-ROM, and a computer system. Furthermore, with "the recording medium in which computer reading is possible." The thing holding a fixed time program shall also be included like the volatile memory (RAM) inside the computer system used as a server when a program is transmitted via communication lines, such as networks, such as the Internet, and a telephone line, or a client.

[0038]The above-mentioned program may be transmitted to other computer systems via a transmission medium from the computer system which stored this program in memory storage etc. by the transmitted wave in a transmission medium. Here, the "transmission medium" which transmits a program says the thing of a medium which has the function to transmit information like communication lines (communication wire), such as networks (communications network), such as the Internet, and a telephone line. The above-mentioned program may be for realizing a part of function mentioned above. They may be what can realize the function mentioned above in combination with the program already recorded on the computer system, and what is called a patch file (difference program).

[0039]As mentioned above, although the embodiment of this invention has been explained in full detail with reference to drawings, concrete composition is not restricted to this embodiment and the design etc. of the range which does not deviate from the gist of this invention are included. Although lessons was taken from a rule, a pattern, etc. and many were illustrated, these are examples to the last and are not this limitation about that format and employment.

[0040]

[Effect of the Invention]Above, like explanation, according to this invention, sources of information are increased and it can utilize as investigative information from the most important methods, such as the existing trespass detecting device, by extending the information made into the object of collection to extensive information including network management information.Therefore, highly precise-ization of NIDS can be attained by performing fine control of the detecting pattern of NIDS and an information acquisition pattern. Suspicious person surveillance is realizable, further, the accuracy of invader detection improves, and quick management is attained [acquisition of more precise invasion information is attained], and wrong detection can also be reduced.

[0041]According to this invention, the effect of enumerating to the following other than the above is also acquired.

(1) The detailed analysis of a "means" is attained and it becomes easy to form the plan corresponding to after the event by using the information just before invasion.

(2) It can investigate by changing a surveillance object and a level dynamically based on the contents of the detected information, without touching ordinary normal users' contents of traffic.

(3) By narrowing down the object which collects information, with few computer resources, it becomes acquirable [information required for next analysis], and reduction of sensor loads can be aimed at.

(4) A regular access person's privacy can be protected by narrowing down the collection object of information to a suspicious person.

consideration of the employment situation of the target network.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－342276
（P2002－342276A）
(43)公開日　平成14年11月29日(2002.11.29)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
G06F	15/00	330	C06F	15/00	330A　5B085
		320			320K　5B089
	13/00	351		13/00	351Z　5K030
H04L	12/22		H04L	12/22	

審査請求　未請求　請求項の数8　ＯＬ　（全 12 頁）

(21)出願番号　特願2001－148024(P2001－148024)

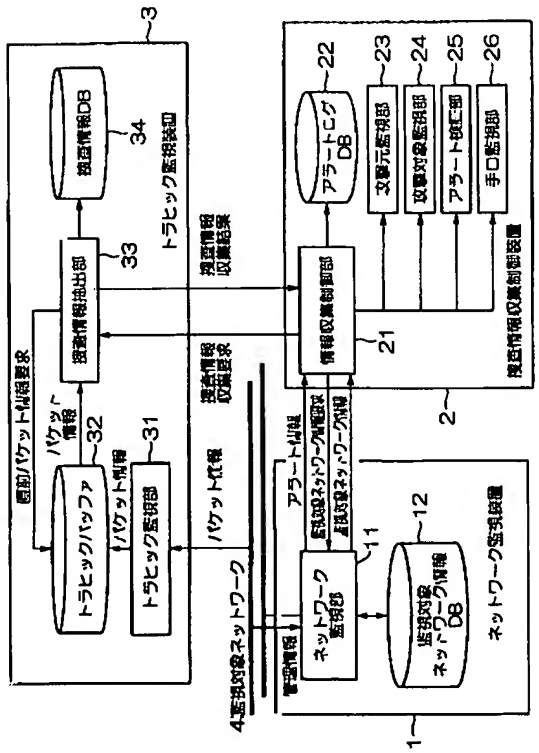
(22)出願日　平成13年5月17日(2001.5.17)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号
(71)出願人　501175281
株式会社サイバー・ソリューションズ
宮城県仙台市青葉区南吉成六丁目6番地の3
(72)発明者　桑田　喜隆
東京都江東区豊洲三丁目3番3号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100064908
弁理士　志賀　正武　（外2名）

最終頁に続く

(54)【発明の名称】　ネットワーク侵入検知システムおよびその方法

(57)【要約】
【課題】　ネットワーク型侵入検知装置の高精度化をはかると共に、情報の収集対象を不審者に絞り込み正規アクセス者のプライバシを保護する。
【解決手段】　予め侵入パターンに応じた複数の検出パターンを準備しておき、捜査情報収集制御装置２により必要に応じてその検出パターンを動的に切替える。また、捜査情報収集制御装置２により、侵入の可能性を示すような軽微な兆候も監視対象とし、そのレベルに応じて監視体制を変更させるべくネットワーク監視装置１およびトラヒック監視装置３を制御する。更に、トラヒック監視装置３で一定量のパケットを常に保持することにより捜査情報収集制御装置２は直前の状態を検査情報として活用する。この保持しているパケットおよび、ネットワーク監視装置１から取得した情報から侵入検知および侵入後の手口の検証を行なう。



【特許請求の範囲】
【請求項１】　監視対象ネットワークからネットワーク管理情報を得、ネットワーク侵入の有無およびその侵入パターンを検知するネットワーク監視装置と、
前記侵入パターンと前記侵入パターンのそれぞれに応じてあらかじめ用意された複数の検知パターンとの照合を行なうことにより該当する検知パターンを動的に切替え、当該検知パターンに従う捜査情報を収集する捜索情報収集制御装置とを備えたことを特徴とするネットワーク侵入検知システム。
【請求項２】　前記捜索情報収集制御装置からの要求に従い、前記検知パターンに従う捜査情報を侵入の直前の情報も含めて出力するトラヒック監視装置を備えたことを特徴とする請求項１に記載のネットワーク侵入検知システム。
【請求項３】　前記捜査情報収集制御装置は、
前記ネットワーク監視装置によって検知された特定の侵入者による通信を集中監視する攻撃元監視部を備えたことを特徴とする請求項１に記載のネットワーク侵入検知システム。
【請求項４】　前記捜査情報収集制御装置は、
前記ネットワーク監視装置によって検知された特定の攻撃対象への通信を集中監視する攻撃対象監視部を備えたことを特徴とする請求項１に記載のネットワーク侵入検知システム。
【請求項５】　前記捜査情報収集制御装置は、
前記ネットワーク監視装置によって検知された検知情報に対し、他に同様の検知情報があるか否かを検証するアラート検証部を備えたことを特徴とする請求項１に記載のネットワーク侵入検知システム。
【請求項６】　前記アラート検証部は、
監視対象ネットワーク情報が格納されたデータベースを参照し、アラート対象ホストの重要度、アラート対象ホストのトラヒック量、アラート対象サービスの重要度の少なくとも１つを前記トラヒック監視装置からの捜査情報の情報取得レベルに反映させることを特徴とする請求項５に記載のネットワーク侵入検知システム。
【請求項７】　前記捜査情報収集制御装置は、
あらかじめその手口シーケンスと手口対抗処理が定義された手口パターンと、前記トラヒック監視装置から得られる侵入元ホストからの捜査情報とを比較することによって手口候補を絞り、当該手口候補が見つかったときにそのターゲットのシャットアウトを含む手口対抗処理を行なう手口監視部を備えたことを特徴とする請求項１、請求項２、請求項５、請求項６のいずれか１項に記載のネットワーク侵入検知システム。
【請求項８】　監視対象ネットワークからネットワーク管理情報を得、ネットワーク侵入の有無およびその侵入パターンを検知し、
前記侵入パターンと前記侵入パターンのそれぞれに応じてあらかじめ用意された複数の検知パターンとの照合を行なうことにより該当する検知パターンを動的に切替え、
当該検知パターンに従う捜査情報を収集することを特徴とするネットワーク侵入検知方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワーク侵入検知システムおよびその方法、詳しくは、ネットワーク侵入の有無を検知するネットワーク型侵入検知装置（ＮＩＤＳ：NetworkIntrusion Detection System）の改良および管理システムとの連携によってセキュリティインシデント前後の情報を詳細に取得する総合的なセキュリティシステムおよびその方法に関する。
【０００２】
【従来の技術】インターネットを活用した企業間取引や顧客へのサービス提供は、戦略的なビジネス展開を模索する企業にとっては最重要課題になっている。しかしながらインターネットの通信環境は、ハッカーによる不正侵入やウイルス感染といった様々な脅威にさらされている。ところで、ファイヤウォールは、企業内ネットワークとインターネットの中間に接続し、インターネットからの不正なアクセスを遮断するセンサとして機能する。ファイヤウォールを設置したネットワークシステムでは、内部から外部へのゲートウェイ的なアクセスを可能にし、インターネットの各種サービスを安全に利用できるようになる。但し、ハッカーによる不正侵入では、ファイヤウォール本体のセキュリティホールを突いた攻撃やポートスキャンによる攻撃、アクセスを妨害する使用不能攻撃等、さまざまな攻撃を受ける危険性がある。
【０００３】
【発明が解決しようとする課題】上記したように、コンピュータシステムの不正利用が大きな社会問題となる中、ネットワーク侵入の有無を検出するネットワーク型侵入検知装置（ＮＩＤＳ）が市販され、応用されるようになってきた。ＮＩＤＳを利用することで、従来の侵入されないことを前提に設計を行なう方法論に対して、侵入される可能性を考慮したネットワークセキュリティシステムを構築することが可能になった。しかしながら従来のＮＩＤＳを用いたネットワークセキュリティシステムによれば、以下に列挙する（１）～（５）の欠点を持つ。
【０００４】（１）予め一義的に定義された検出パターンに従った検出しか行なうことができず、従って、誤検出が多い。
（２）侵入手口の高度化とともに、その検出定義パターンが複雑になり、定義の記述が困難である。
（３）ＮＩＤＳは、不正であると定義されたパケットのみを検知するため、不正検知前後の攻撃者の一連の行動を監視するために必要な情報を取得することができなか

った。また、複数ステップから成る「手口」を記録するためには、ＮＩＤＳで不正を検出後、ＮＩＤＳと独立なパケット監視・記録装置を動作させるしか手立てがなく、迅速に詳細な情報を取得することができなかった。更に、脅威の程度に応じた動的な監視体制を構築することができず、常に侵入に関する詳細な情報をとろうとすれば、ディスク、ＣＰＵ等、パケット監視・記録装置に多くの計算機リソースが必要であると同時に、収集した膨大な情報の解析は事実上不可能であった。

（４）侵入が検出された場合、その結果が未知の侵入であるか、または誤検出か否かを検証することが困難であった。検出結果の検証を行なうためには、予め詳細情報の取得を行う設定にしておく必要があり、検出後詳細情報を取得するように変更しても、多くの場合、既に侵入が終わっているため手遅れとなっていた。

（５）情報収集のために正規アクセス者のプライバシを侵害する恐れがあった。

【０００５】本発明は上記事情に鑑みてなされたものであり、予め侵入パターンに応じた複数の検出パターンを準備しておき、必要に応じてこれを動的に切替え、その詳細情報を取得する仕組みを用意することで情報源を増やして捜査情報として活用し、かつ、トラヒック監視装置と連携してその詳細情報を入手することによりＮＩＤＳの高精度化をはかったネットワーク侵入検知システムおよびその方法を提供することを目的とする。また、侵入の可能性を示すような軽微な兆候も監視対象とし、そのレベルに応じてネットワーク監視体制を変更させることにより、情報の収集対象を不審者に絞り込み、正規アクセス者のプライバシを保護するネットワーク侵入検知システムおよびその方法を提供することも目的とする。

【０００６】

【課題を解決するための手段】上記した課題を解決するために本発明は、監視対象ネットワークからネットワーク管理情報を得、ネットワーク侵入の有無およびその侵入パターンを検知するネットワーク監視装置と、前記侵入パターンと前記侵入パターンのそれぞれに応じてあらかじめ用意された複数の検知パターンとの照合を行なうことにより該当する検知パターンを動的に切替え、当該検知パターンに従う捜査情報を収集する捜索情報収集制御装置とを備えたことを特徴とする。

【０００７】また、本発明において、前記捜索情報収集制御装置からの要求に従い、前記検知パターンに従う捜査情報を侵入の直前の情報も含めて出力するトラヒック監視装置を備えたことを特徴とする。

【０００８】また、本発明において、前記捜査情報収集制御装置は、前記ネットワーク監視装置によって検知された特定の侵入者による通信を集中監視する攻撃元監視部を備えたことを特徴とする。

【０００９】また、本発明において、前記捜査情報収集制御装置は、前記ネットワーク監視装置によって検知された特定の攻撃対象への通信を集中監視する攻撃対象監視部を備えたことを特徴とする。

【００１０】また、本発明において、前記捜査情報収集制御装置は、前記ネットワーク監視装置によって検知された検知情報に対し、他に同様の検知情報があるか否かを検証するアラート検証部を備えたことを特徴とする。

【００１１】また、本発明において、前記アラート検証部は、監視対象ネットワーク情報が格納されたデータベースを参照し、アラート対象ホストの重要度、アラート対象ホストのトラヒック量、アラート対象サービスの重要度の少なくとも１つを前記トラヒック監視装置からの捜査情報の情報取得レベルに反映させることを特徴とする。

【００１２】また、本発明において、前記捜査情報収集制御装置は、あらかじめその手口シーケンスと手口対抗処理が定義された手口パターンと前記トラヒック監視装置から得られる侵入元ホストからの捜査情報とを比較することによって手口候補を絞り、当該手口候補が見つかったときにそのターゲットのシャットアウトを含む手口対抗処理を行なう手口監視部を備えたことを特徴とする。

【００１３】上記構成において、予め侵入パターンに応じた複数の検出パターンを準備しておき、必要に応じて動的に切替える仕組みを用意することにより、収集の対象とする情報を既存のＮＩＤＳによる一義的な方式から、ネットワーク管理情報を含めた広範な情報に拡張することで情報源を増やし捜査情報として活用することができる。また、ＮＩＤＳの検出パターンおよび情報取得パターンの細かなコントロールを行なうことで、ＮＩＤＳの高精度化が図れる。更に、トラヒック監視装置で一定量のパケットを常に保持することにより、捜査情報収集制御装置は直前の状態も含めて検知情報として活用できる。従って、この保持しているパケットおよび、上記により取得した情報からの侵入検査および侵入後の手口の検証が可能になる。また、捜査情報収集制御装置により、侵入の可能性を示すような軽微な兆候も監視対象とし、そのレベルに応じて監視体制を変更させることができる。具体的には、必要に応じてトラヒック監視装置対して指示を出し、その情報取得レベルを動的に変更し、その結果、情報の収集対象を不審者に絞り込むことになり、正規アクセス者のプライバシを保護することができる。

【００１４】上記した課題を解決するために本発明は、監視対象ネットワークからネットワーク管理情報を得、ネットワーク侵入の有無およびその侵入パターンを検知し、前記侵入パターンと前記侵入パターンのそれぞれに応じてあらかじめ用意された複数の検知パターンとの照合を行なうことにより該当する検知パターンを動的に切替え、当該検知パターンに従う捜査情報を収集することを特徴とする。

【００１５】また、本発明において、前記検知パターンに従う捜査情報を侵入の直前の情報も含めて出力することを特徴とする。

【００１６】

【発明の実施の形態】図１は、本発明におけるネットワーク侵入検知システムの一実施形態を示すブロック図である。本発明のネットワーク侵入検知システムは、ネットワーク監視装置１と、捜査情報収集制御装置２と、トラヒック監視装置３と、監視対象ネットワーク４で構成される。ネットワーク監視装置１は、監視対象ネットワーク４からネットワーク管理情報を得、ネットワーク侵入の有無およびその侵入パターンを検知する機能を有する。また、捜査情報収集装置２は、侵入パターンと侵入パターンのそれぞれに応じてあらかじめ用意された複数の検知パターンとの照合を行なうことにより該当する検知パターンを動的に切替え、当該検知パターンに従う捜査情報を収集する機能を有する。更に、トラヒック監視装置３は、捜索情報収集制御装置２からの要求に従い、検知パターンに従う捜査情報を侵入の直前の情報も含めて出力する機能を有する。

【００１７】ネットワーク監視装置１は、ネットワーク監視部１１と、監視対象ネットワーク情報ＤＢ（データベース）１２で構成される。ネットワーク監視部１１は、監視対象ネットワーク４からネットワーク管理情報を得、不正侵入を検知することにより捜査情報収集制御装置２に対して検知情報（アラート情報）を伝え、捜査情報収集制御装置２からの監視対象ネットワーク情報要求に基づき監視対象ネットワーク情報ＤＢ１２に蓄積された監視対象ネットワーク情報を提供する。監視対象ネットワークＤＢ１２には、ネットワーク構成情報、サービス情報、運用情報の他に、ヘッダとペイロード（内容）から構成されるＩＰパケット情報が蓄積される。なお、ネットワーク構成情報としては、ネットワークに接続されたホスト、ルータ等の機器の詳細ルーティング情報が、サービス情報としては、ホストのサービス提供ポリシー、実際にホストに提供するサービスが、運用情報としては、ホスト毎のトラヒック情報、サービス毎のトラヒック情報（アクセス頻度）が蓄積される。なお、監視対象ネットワークＤＢ１２には、ホストおよびサービスの重要度、トラヒック量の高低に関する情報も含まれ、その一例が図６、図７に示されている。また、ここでは、監視対象ネットワーク情報ＤＢ１２がネットワーク監視装置１内にあるものとして説明するが、後述する捜査情報収集制御装置２にあってもよい。この場合、基本的な制御部が全て捜査情報収集装置２に集められるため、ネットワーク監視装置１の構成および機能をシンプルにすることが可能である。

【００１８】捜査情報収集制御装置２は、情報収集制御部２１を核に、アラートログＤＢ（データベース）２２と、攻撃元監視部２３と、攻撃対象監視部２４と、アラート検証部２５と、手口監視部２６で構成される。情報収集制御部２１は、ネットワーク監視装置１からのアラート情報によって起動され、攻撃元監視部２３、攻撃対象監視部２４、アラート検証部２５、手口監視部２６とのインタフェースを司り、トラヒック監視装置３から該当する捜査情報の収集を開始するものであり、図２に示されるように、ルール解析部２１１と、パターンマッチ部２１２と、アクション実行部２１３と、ルールライブラリ２１４で構成される。

【００１９】捜査情報収集装置２に侵入パターンのそれぞれに応じて複数の検知パターンがあらかじめ用意されることは上記した通りである。ここではその検知パターンがルールとしてライブラリ化されており、ルールライブラリ２１４中に記憶されている。ルール解析部２１１がこのルールを読み取って解析を行い、パターンマッチ部２１２でネットワーク監視部１を介して得られるＩＰパケットと照合し、一致のとれた検知パターンに従うアクションをアクション実行部２１３で実行する。ここでいうアクションとは、トラヒックの記録開始、中止、特定攻撃元監視、特定対象監視、アラート検証、手口監視であり、必要に応じてルールセットの変更を行なう。

【００２０】図３、図４に、それぞれ、ルール書式、ルールの一例を示す。図３（ａ）に示されるように、ルールは、”パターン”部と”アクション”部によって定義される。パターンとして、ｔｃｐ（transfer control protocol）、ｕｄｐ（userdatagram protocol）等のプロトコル（protocol）、ＩＰアドレス、ポート番号等のソース仕様（source-spec）、双方向／片方向（<¦>）、ＩＰアドレス、ポート番号等のデステネーション仕様（dest-spec）、その他ペイロード部のマッチング仕様（matchinf-spec）等が記述される。なお、図中＊印は繰り返しを意味する。

【００２１】図３（ｂ）はパターン部の書式を表したものであり、上記したＩＰアドレスとポート番号の他に、タイトル値（ttl）、ＩＣＭＰ（Internet Control Message Protocol）タイプ（itype）、ＩＣＭＰコード（icode）、最小フアラグメントペイロードサイズ（minfrag）、ＴＣＰシーケンス番号（seq）、ＴＣＰ－ＡＣＫ（Acknowledge）番号（ack）、ＩＰヘッダのフラグメントＩＤ番号（id）、ペイロードサイズ（dsize）、パターンマッチ用のパケットの内容（content）がある。図３（ｃ）は、アクション情報を表したものであり、アラート情報を上位装置のマネージャ（情報収集制御部２１）に送るアラート（alert）、メッセージをログファイルに格納するログ（log）、ルールセットを切替えるフォークルールセット（fork-ruleset）、トラヒック監視装置３の制御を行うレコード（record）等がある。

【００２２】図４は、図３に示した書式に従い、攻撃元監視を行なう場合、攻撃対象監視を行なう場合、ポートスキャンを検出したときに攻撃元監視を行う場合の、そ

れぞれのルール例を示したものである。攻撃元監視では、ルールネーム”sniffing-host”において、任意プロトコルでＩＰアドレス”192.168.10.10”の任意ポートを監視して変数$HOME_NETの任意ポートに全て記録することを意味し、攻撃対象監視では、ルールネーム”watch-home”において、任意プロトコル、任意ＩＰアドレス、任意ポートを監視してＩＰアドレス”192.168.0.5”の任意ポートに、全てのヘッダ情報に加えペイロード頭２０バイトを記録することを意味する。また、ポートスキャンを検出したときに攻撃元監視を行う場合、ルールネーム”switch-snif”において、任意プロトコルで任意ＩＰアドレスの任意ポートを監視して変数$HOME_NETの任意ポートスキャン検出後、変数$source_addressにある”snifing-host”にルールセットを切替えることを意味する。

【００２３】説明を図１に戻す。攻撃元監視部２３は、ネットワーク監視装置１によって検知された特定の侵入者による通信を集中監視する機能を有し、攻撃対象監視部２４は、ネットワーク監視装置１によって検知された特定の攻撃対象への通信を集中監視する機能を有する。また、アラート検証部２５は、ネットワーク監視装置１によって検知された検知情報に対し、他に同様の検知情報があるか否かを検証する機能を有する。更に、手口監視部２６は、監視対象ネットワーク情報ＤＢ１２を参照し、アラート対象ホストの重要度、アラート対象ホストのトラヒック量、アラート対象サービスの重要度の少なくとも１つをトラヒック監視装置２からの捜査情報の情報取得レベルに反映させると共に、あらかじめその手口シーケンスと手口対抗処理が定義された手口パターンとトラヒック監視装置２から得られる侵入元ホストからの履歴を示す捜査情報とを比較することによって手口候補を絞り、当該手口候補が見つかったときにそのターゲットのシャットアウトを含む手口対抗処理を行なう機能を有する。なお、攻撃元監視部２３、攻撃対象監視部２４についての具体的事例は図４に示したとおりであり、アラート検証部２５、手口監視部２６についての詳細は具体的事例を用いて後述する。

【００２４】トラヒック監視装置３は、トラヒック監視部３１と、トラヒックバッファ３２と、捜査情報抽出部３３と、捜査情報ＤＢ（データベース）３４で構成される。トラヒック監視部３１は、監視対象ネットワーク４から得られる一定量のパケットを常時トラヒックバッファ３２に蓄積する機能を有する。トラヒックバッファ３２はＦＩＦＯ（First-In First-Out）方式のバッファであって、捜査情報抽出部３３からのパケット情報要求に基づき、既に蓄積してあるパケット情報を所定の単位毎転送する。捜査情報抽出部３３は、転送されたパケット情報を捜査情報ＤＢ３４に蓄積すると共に、捜査情報収集制御装置２から発せられる捜査情報収集要求に基づき、その要求した情報取得レベルに応じた詳細情報を捜査情報ＤＢ３４を検索することにより供給する機能も合わせ持つ。

【００２５】図５は、図１に示す捜査情報収集制御装置２の動作につき、ネットワークセキュリティシステムを例示して示した動作概念図である。ここでは、ネットワーク監視装置１－１で監視ネットワーク４－１のサーバ５－１に対する侵入検知情報と関連情報を検知し、捜査情報収集制御装置２に通知する（①）。捜査情報収集制御装置２は、関連のリンクの監視を強化するためにネットワーク監視装置１－２、ネットワーク監視装置１－３をグルーピングしてネットワーク監視装置１－１で検知されたソースアドレス情報等を基準として集中的に監視するように指示を発する（②）。同時にネットワーク監視装置１－２、１－３では「手口」に関する情報を収集する（③）。また、監視ネットワーク４－１とは異なるネットワーク４－２に対する攻撃を事前に警戒することを実現するために直接関連のないネットワーク監視装置１－４に対しても③で判明した手口が利用されているか否かを監視し、早期警戒に努めている（④）。

【００２６】以下、図６以降を参照しながらアラート検証、手口監視について説明する。図６、図７は、アラート検証処理の流れをフローチャートで示したものであり、また、図８は、アラート検証処理の入出力例を概念的に示したものである。まず、図６に示すフローチャートにおいて、アラート関連情報として、対象ＯＳ、対象ネットワークサービス、対象バージョン、対象パッチレベル他が設定されていることを前提に、アラート検証部２５は、まず、対象ホスト情報を監視対象ネットワーク情報ＤＢ１２から取得する（ステップＳ６１）。また、アラート検証部２５は、アラート対象ＯＳは攻撃対象ＯＳと等しいか否かをチェックし（ステップＳ６２）、等しくないと判定された場合は無効アラート処理を（ステップＳ６３）、等しいと判定された場合は、更に、アラート対象ネットワークサービスが攻撃対象ホストで動作中か否かをチェックする（ステップＳ６４）。

【００２７】ここで、アラート対象ネットワークサービスが攻撃ホストで動作中でないと判定された場合には、更にネットワークサービス検証処理（ステップＳ６５）を、動作中と判定された場合には、更にアラート対象ネットワークサービスのバージョンが攻撃対象ホストと同一か否かがチェックされる（ステップＳ６６）。ネットワークサービス検証処理を行なう（ステップＳ６５）ことでアラート対象ネットワークサービスが攻撃対象ホストで現時点で動作中か否かを判定し（ステップＳ６１０）、動作中でない場合にはステップＳ６１２で無効アラート処理を行い、動作中であった場合は、ステップＳ６１１で不正サービス処理を行なう。なお、アラート対象ネットワークサービスのバージョンが攻撃対象ホストで動作中のものと異なると判定された場合は無効アラート処理（ステップＳ６７）を、等しいと判定された場合

は図7に示す有効アラート処理を開始する（ステップS68）。そして、攻撃対象ホストの全てが終了するまで上記したステップS61からS68に至るアラート検証処理を繰り返す（ステップS69）。

【0028】図7に示すフローチャートにおいて、アラート検証部25は、監視対象ネットワーク情報DB12に定義されてあるアラート対象ホストの重要度をチェックし、あらかじめ設定された閾値と比較して重要度が高いと判定された場合にその重要度を＋1更新する処理を行う（ステップS72）。重要度がそれほど高くない場合は更に監視対象ネットワーク情報DB12を参照してアラート対象ホストトラヒック量をチェックし、高いと判定された場合、先の重要度同様トラヒック量の重要度を＋1更新する。トラヒック量がそれほど高くない場合は更にアラート対象サービスの重要度をチェックし、重要度が高い場合にその重要度を＋1更新する。重要度がそれほど高くない場合に有効アラート処理を終了する。ここでアラート検証部25が単なるアラート検証処理の他に重要度を制御する理由は、トラヒック監視装置3を制御して詳細情報を収集するときのレベル判断に使用するためである。

【0029】図8にアラート検証のための入出力例が示されている。図8において、アラート検証部25は、まず、ネットワーク監視部1から情報収集制御部21を介してアラート情報を入力情報として受信する。入力情報は、IDが"1080"、アラート対象ホストのアドレスが"192.168.0.1"、種類が"SNMP public access"、ネットワークサービス名が"SNMP：Simple Network Management Protocol"、ポート番号が"161"、バージョンが任意バージョンから成るアラート情報#1、IDが"1080"、アラート対象ホストのアドレスが"192.168.0.1"、種類が"anonymous ftp"、ネットワークサービス名が"FTP：File Transfer Protocol"、ポート番号が"21"、バージョンが任意バージョンから成るアラート情報#2である。一方、攻撃対象ネットワーク情報DB260には、ホストが"192.168.01"、ネットワークサービス名が"SNMP"、バージョン"2.0"、ステイタスを"ACTIVE"とする攻撃対象ネットワーク情報#1が、ホストが"192.168.01"、ネットワークサービス名が"SNMP"、バージョン"2.0"、ステイタスを"ACTIVE"、ネットワークサービス名を"FTP"、バージョンを"3.0"、ステイタスを"INACTIVE"とする攻撃対象ネットワーク情報#2が格納されている。ここで検証の結果、アラート情報#1については有効アラート処理を、アラート情報#2については出力項目として無効アラート処理を実行することになる。

【0030】図9、図10は、手口監視部26による手口監視の例を示したものであり、それぞれ、処理の流れをフローチャートで、手口パターンの例をリスト形式で記述したものである。図10に示されるように、ここでは、（1）から（4）で示す4通りの手口パターンが例示されており、それぞれに手口シーケンスと手口対抗処理が示されている。すなわち、手口パターン（1）では、ポートスキャンがあってウェッブCGIに対する攻撃によりバッファオーバフローが検出される3つの手口シーケンスの対抗処理として、その攻撃元ホスト（source）のシャットダウンと"ターゲットホストはソースによって侵入された"旨のアラートが発せられる。手口パターン（2）では、ポートスキャンがあって、"finger"および"telnet"サービスの後、バッファオーバフローが検出された4つのシーケンスの対抗処理として、その相手先（source）のシャットアウトと"ターゲットホストはソースによって侵入された"旨のアラートが発せられる。

【0031】一方、手口パターン（3）は、複数ホストからの攻撃手口が検出された場合を示し、複数ホスト（Other_Hosts）から対象ホスト（target）への分散DOS攻撃を検出し、引き続き相手先ホスト（Source）から対象ホストへのPing_Of_Death攻撃を検出した場合、その対抗措置として相手先ホスト、複数ホストのシャットアウト、および"ターゲットホストはソースホストにより侵入された"旨のアラートが発せられる。また、手口パターン（4）も複数ホスト（Other_Hosts）からDNSを実行する対象ホスト（DNS_SERVER）への分岐DOS攻撃を検出し、同時にDNS（Domain Name Server）として登録されていないホストからのDNS対応メッセージを確認した場合、相手先ホスト、複数ホストのシャットアウトおよび"DNSサーバがダウンした"旨のアラートが発せられる。

【0032】図9に示すフローチャートにおいて、手口監視部26は、アラート情報を受信後、手口パターンDB270から手口パターンを取得する（ステップS91）。手口パターンとして、図10に示したように対抗シーケンスとその対抗処理が記述されている。手口監視部26はまた捜査情報DB34を参照することにより攻撃元ホスト（source）からの履歴情報を取得する（ステップS92）。そして、複数ホストからの手口の場合、手口監視部26は更に、その他ホストからの履歴情報を取得して（ステップS93）、手口パターンと履歴の照合を行なう（ステップS94）。ここで、一致した場合は手口候補を絞り（ステップS95）、不一致の場合はステップS91の処理に戻って次の手口パターン情報を取得し、以降、手口パターンが継続するまで上記の操作を繰り返す（ステップS96）。そして、手口候補が絞られたときに（ステップS97）、手口パターンDB270に手口対抗として記述された処理を行なう。すなわち、図10に記述されるように、例えば、攻撃元ホスト（source）のシャットアウトと"ターゲットホストはソースによって侵入された"旨のアラートが発せられ、また、複数ホストからの攻撃手口が検出された場合に、例

えば、相手先を含む他のホストのシャットアウトおよび”ＤＮＳサーバがダウンした”旨のアラートが発せられる。

【００３３】以上説明のように本発明によれば、ＮＩＤＳおよび管理システムとの連携によりセキュリティインシデント前後の情報を詳細に取得する総合的なセキュリティシステムを構築することができる。また、予め侵入パターンに応じた複数の検出パターンを準備しておき、必要に応じて動的に切替える仕組みを用意することにより、収集の対象とする情報を既存のＮＩＤＳによる一義的な方式から、ネットワーク管理情報を含めた広範な情報に拡張することで情報源を増やし捜査情報として活用することができる。また、ＮＩＤＳの検出パターンおよび情報取得パターンの細かなコントロールを行なうことで、ＮＩＤＳの高精度化が図れる。具体的には、全ポートに対するポートスキャンを検出し、その後、同じホストから例えばsmtpポートに対する不穏なアクセスを検出したら、smtpの脆弱性に関する侵入検査パターンを重点的に適用する様に、ＮＩＤＳのルールを切替える。

【００３４】また、捜査情報収集制御装置２により、侵入の可能性を示すような軽微な兆候も監視対象とし、そのレベルに応じて監視体制を変更させる。具体的には、必要に応じてトラヒック監視装置３対して指示を出し、その情報取得レベルを動的に変更し、その結果、情報の収集対象を不審者に絞り込むことになり、正規アクセス者のプライバシを保護することができる。例えば、あるステップで、ＮＩＤＳによりあるＩＰアドレスからの侵入に向けた不穏な動きが検出された場合、そのＩＰアドレスからのある特定ポートに対する全パケットに対して、先頭からｎビット分を記録する。そして次のステップで、そのＩＤアドレスからの不穏な動きが継続してｎ分以上検出された場合、そのＩＤアドレスからの全ポートに対する全パケットの先頭からｎビット分を記録し、更に次のステップでそのＩＤアドレスからの侵入可能性が検出された場合、そのＩＤアドレスのパケットを全て記録する。

【００３５】更に、トラヒック監視装置３で一定量のパケットを常に保持することにより捜査情報収集制御装置２は直前の状態を検査情報として活用できる。この保持しているパケットおよび、上記により取得した情報からの侵入検査および侵入後の手口の検証が可能になる。例えば、ＩＰアドレス”10.2.190.38”からの通信内容の全記録から、ポート”25”に対する”smtp”での侵入を試みた形跡が見つかったが、侵入は失敗に終わったことが判明し、また、先のポート”25”以外に対する通信記録を調べたところ、ポート”80”の”cgi”に対する見慣れないフォーマットによる通信が、先の例に次いで多いことが判明した場合、結果として、ポート”80”の”cgi”に対する未知の侵入方法を試みたことが判明する。

【００３６】なお、上記したネットワーク監視装置１と、捜査情報収集制御装置２と、トラヒック監視装置３と、ネットワーク監視部１１と、情報収集制御部２１と、攻撃元監視部２３と、攻撃対象監視部２４と、アラート検証部２５と、手口監視部２６と、トラヒック監視部３１と、操作情報抽出部３３と、ルール解析部２１１と、パターンマッチ部２１２と、アクション実行部２１３のそれぞれで実行される手順をコンピュータ読み取り可能な記録媒体に記録し、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより上述した各装置における機能を実行してもよい。ここでいうコンピュータシステムとは、ＯＳや周辺機器等のハードウアを含むものとする。

【００３７】また、「コンピュータシステム」は、ＷＷＷシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。

【００３８】また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【００３９】以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。また、ルールやパターン等につき数多く例示したが、これらはあくまで一例であってそのフォーマットならびに運用についてはこの限りでない。

【００４０】

【発明の効果】以上説明のように本発明によれば、収集の対象とする情報を既存の侵入検知装置等の一義的な方式から、ネットワーク管理情報を含めた広範な情報に拡張することで、情報源を増やし捜査情報として活用でき

る 従って、ＮＩＤＳの検出パターンおよび情報取得パターンの細かなコントロールを行うことで、ＮＩＤＳの高精度化が図れる。また、より緻密な侵入情報の取得が可能になり、不審者監視が実現でき、更に、侵入者検知の精度が向上し、かつ迅速な対処が可能となり、誤検知も削減することができる。

【００４１】本発明によれば、上記の他に以下に列挙する効果も得られる。

（１）侵入の直前情報を利用することにより、「手口」の詳細な解析が可能となり、事後対応計画が立てやすくなる。

（２）検知した情報の内容に基づき監視対象、およびレベルを動的に変更することで、一般の正規利用者のトラヒック内容に触れずに調査することができる。

（３）情報を収集する対象を絞り込むことにより、少ない計算機リソースで、後の解析に必要な情報の取得が可能となり、センサ負荷の削減がはかれる。

（４）情報の収集対象を不審者に絞り込むことにより、正規アクセス者のプライバシを保護できる。

（５）詳細な侵入検知情報の取得をきめ細かく制御できるため安価な機材を用いてシステム構築が可能となる。

（６）侵入情報を検知した後、対象となるネットワークの運用状況を考慮して侵入検知情報の検証を行なうことが可能である。

【図面の簡単な説明】

【図１】　本発明におけるネットワーク侵入検知システムの一実施形態を示すブロック図である。

【図２】　図１に示す情報収集制御部の内部構成を示すブロック図である。

【図３】　ルールライブラリに記述されるルール書式を説明するために引用した図である。

【図４】　図２に示すルールライブラリに格納されたルールの一例を示す図である。

【図５】　図１に示す捜査情報収集制御装置の動作につき、ネットワークセキュリティシステムを例示して示した動作概念図である。

【図６】　アラート検証処理の流れをフローチャートで示した図である。

【図７】　図６に示す有効アラート処理の詳細な流れをフローチャートで示した図である。

【図８】　アラート検証処理を説明するために引用した動作概念図である。

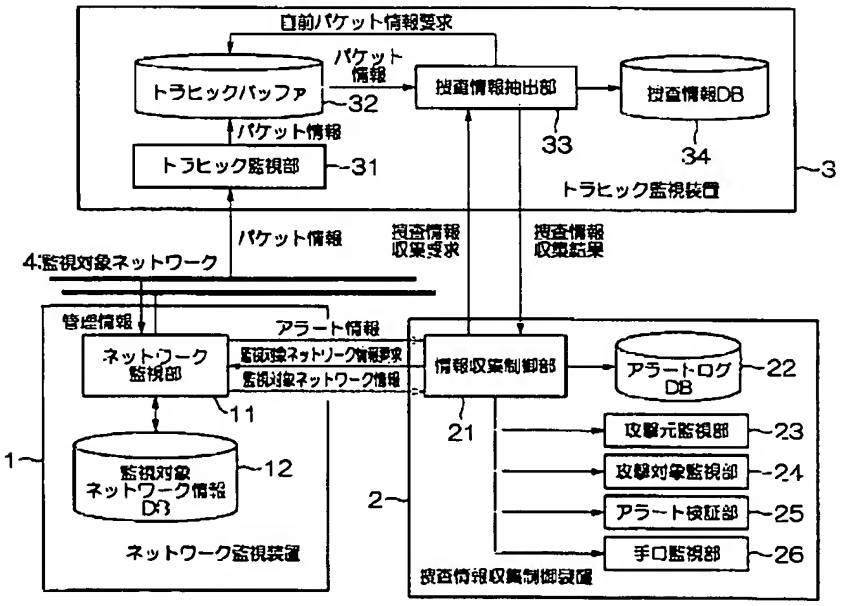
【図９】　手口監視処理の流れをフローチャートで示した図である。

【図１０】　手口監視のために手口パターンＤＢに記述される手口パターンの例を示す図である。

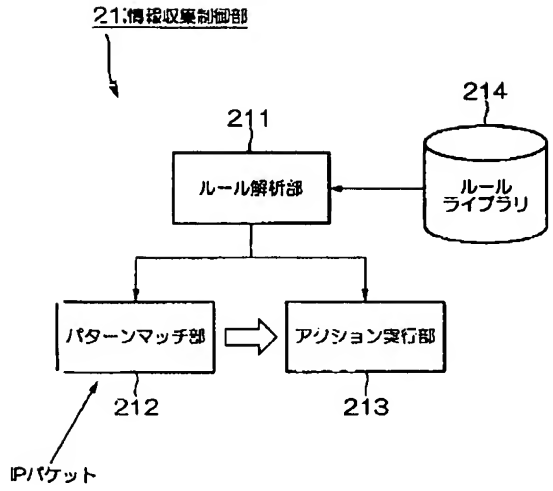
【符号の説明】

１…ネットワーク監視装置、２…捜査情報収集制御装置、３…トラヒック監視装置、４…監視対象ネットワーク、１１…ネットワーク監視部、１２…監視対象ネットワーク情報ＤＢ、２１…情報収集制御部、２２…アラートログＤＢ、２３…攻撃元監視部、２４…攻撃対象監視部、２５…アラート検証部、２６…手口監視部、３１…トラヒック監視部、３２…トラヒックバッファ、３３…捜査情報抽出部、３４…捜査情報ＤＢ、２１１…ルール解析部、２１２…パターンマッチ部、２１３…アクション実行部

【図１】



【図2】



【図3】

(a)

ルールの書式

rule := [pattern] actions
pattern := protocol source spec (<> | ->) dest-spec [matching-spec*]
protocol := {tcp|udp|any}
source-spec := ip address port-no
dest-spec := ip-address port-no
ip-address := {IP Address | IP Address Range | any}
port-no := {NUMBER | NUMBER_LO:NUMBER_HI}

ruleset := ruleset rulename { rule * }

(b)

パターン部の書式
（ヘッダ情報）
ttl : TTL値
itype : ICMP type
icode : ICMP code
minfrag : 最小フラグメントペイロードサイズ
seq : TCP シーケンス番号
ack : TCP ACK番号
id : IPヘッダーのフラグメントID番号
（ペイロード情報）
dsize : ペイロードサイズ
content : パケットの内容（パターンマッチ）

(c)

アクション情報
alert : アラートをマネージャに送る
log : メッセージをログファイルに格納する
fork-ruleset : ルールセットを切り替える
record : トラヒック監視装置の制御を行う

【図4】

```
攻撃元監視
ruleset snifing-host {
[any 192.168.10.10 any -> $HOME_NET any] record(all)
}

攻撃対象監視
ruleset watch-home {
[any any any -> 192.168.0.5 any] record(header+20byte)
}

ポートスキャンを検出した場合に攻撃元監視を開始する
ruleset switch-snif {
[any any any -> $HOME_NET any port-scan-detected]
    fork-ruleset snifing-host($source0address)
}
```

【図10】

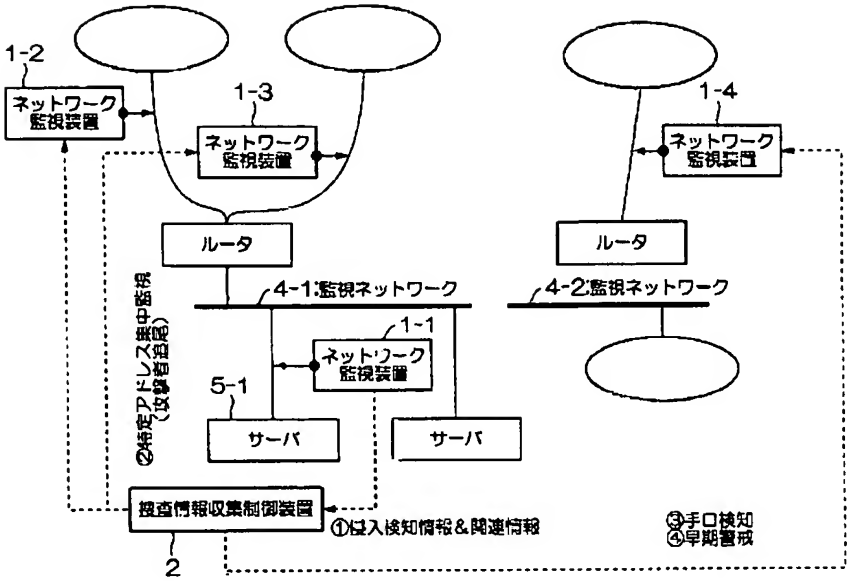
手口パターン（1）
シーケンス：Port-scan(source, target),
　　Web-cgi (source, target),
　　buffer_overflow(source, target)
対抗処理：Shutout(source),
　　Alert("target is intruded by source")

手口パターン（2）
シーケンス：Port-scan(source, target),
　　finger(source, target),
　　telnet(source, target),
　　buffer_overflow(source, target)
対抗処理：Shutout(source),
　　Alert("target is intruded by source")

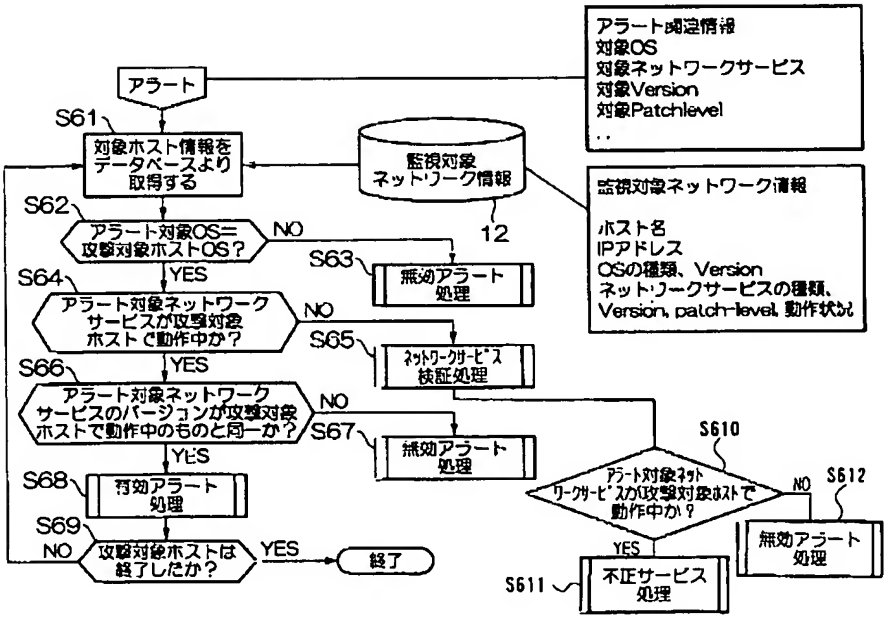
手口パターン（3）複数ホストからの攻撃手口
シーケンス：DDOS(Other_Hosts, target),
　　Ping_Of_Death(source, target)
対抗処理：Shutout($OtherHosts),
　　Shutout(source),
　　Alert("target is intruded by source");

手口パターン（4）
シーケンス：DDOS(OtherHosts, DNS_SERVER),
　　false_DNS_reply(source)
対抗処理：Shutout(OtherHosts),
　　Shutout(source),
　　Alert("DNS_SERVER is down")

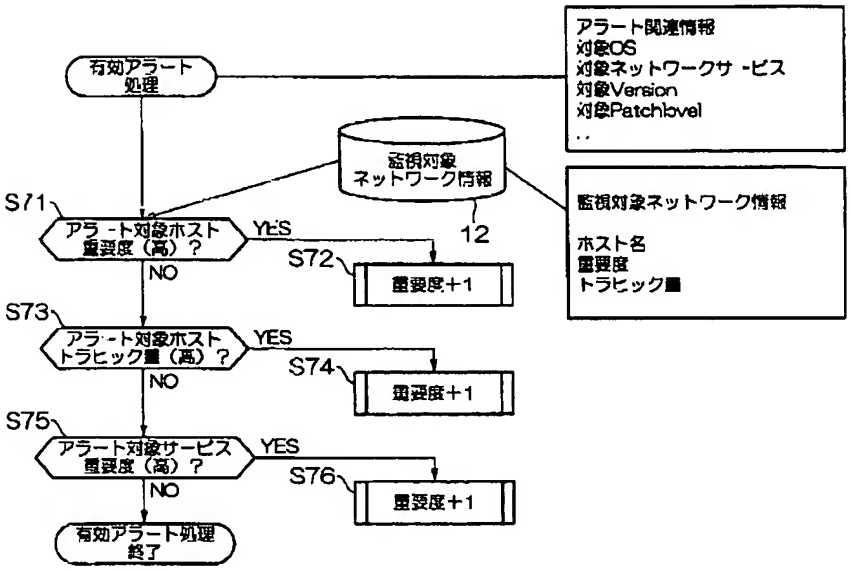
【図5】


1-2
ネットワーク監視装置
1-3
ネットワーク監視装置
1-4
ネットワーク監視装置
ルータ
ルータ
4-1:監視ネットワーク
4-2:監視ネットワーク
1-1
ネットワーク監視装置
5-1
サーバ
サーバ
②特定アドレス集中監視(攻撃者追跡)
検査情報収集制御装置
①侵入検知情報&関連情報
③手口検知
④早期警戒
2

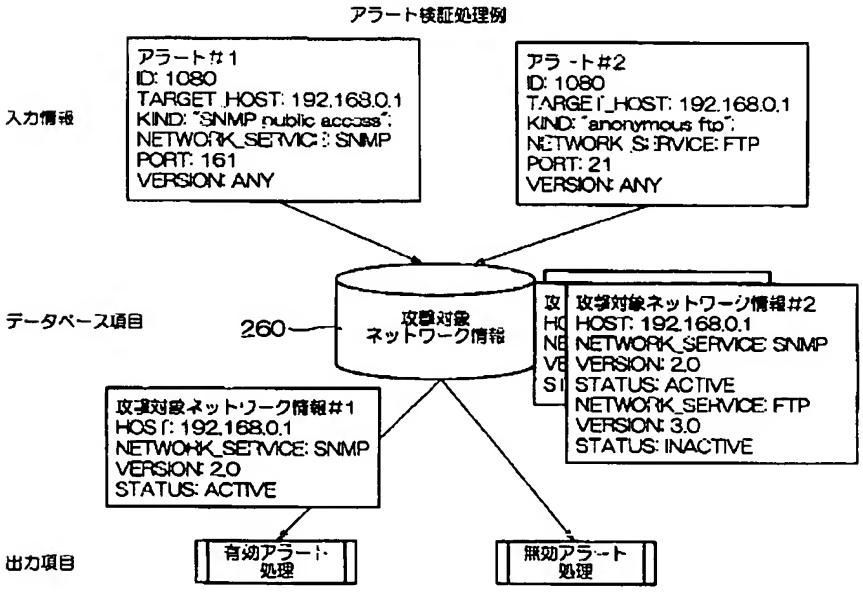
【図6】


アラート関連情報
対象OS
対象ネットワークサービス
対象Version
対象Patchlevel
..
アラート
S61
対象ホスト情報をデータベースより取得する
監視対象ネットワーク情報
12
監視対象ネットワーク情報
ホスト名
IPアドレス
OSの種類、Version
ネットワークサービスの種類、Version、patch-level、動作状況
S62
アラート対象OS=攻撃対象ホストOS?
NO
S63
無効アラート処理
YES
S64
アラート対象ネットワークサービスが攻撃対象ホストで動作中か?
NO
S65
ネットワークサービス検証処理
YES
S66
アラート対象ネットワークサービスのバージョンが攻撃対象ホストで動作中のものと同一か?
NO
S67
無効アラート処理
YES
S68
有効アラート処理
S69
NO
攻撃対象ホストは終了したか?
YES
終了
S610
アラート対象ネットワークサービスが攻撃対象ホストで動作中か?
NO
S612
無効アラート処理
YES
S611
不正サービス処理

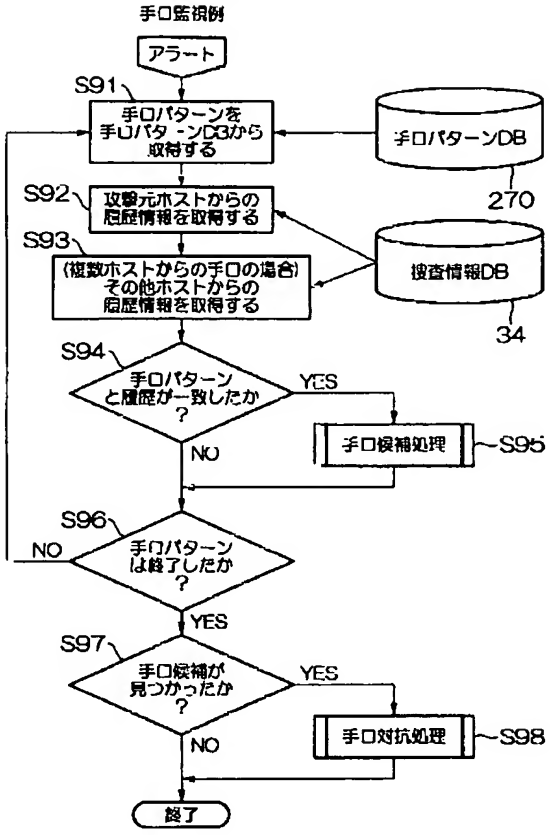
【図7】


有効アラート処理
アラート関連情報
対象OS
対象ネットワークサービス
対象Version
対象Patchlevel
監視対象ネットワーク情報
12
監視対象ネットワーク情報
ホスト名
重要度
トラヒック量
S71
アラート対象ホスト重要度（高）？
YES
S72
重要度+1
NO
S73
アラート対象ホストトラヒック量（高）？
YES
S74
重要度+1
NO
S75
アラート対象サービス重要度（高）？
YES
S76
重要度+1
NO
有効アラート処理終了

【図8】


アラート検証処理例
入力情報
アラート#1
ID: 1080
TARGET_HOST: 192.168.0.1
KIND: "SNMP public access"
NETWORK_SERVICE: SNMP
PORT: 161
VERSION: ANY
アラート#2
ID: 1080
TARGET_HOST: 192.168.0.1
KIND: "anonymous ftp"
NETWORK_SERVICE: FTP
PORT: 21
VERSION: ANY
データベース項目
260
攻撃対象ネットワーク情報
攻撃対象ネットワーク情報#2
HOST: 192.168.0.1
NETWORK_SERVICE: SNMP
VERSION: 2.0
STATUS: ACTIVE
NETWORK_SERVICE: FTP
VERSION: 3.0
STATUS: INACTIVE
攻撃対象ネットワーク情報#1
HOST: 192.168.0.1
NETWORK_SERVICE: SNMP
VERSION: 2.0
STATUS: ACTIVE
出力項目
有効アラート処理
無効アラート処理

【図9】



フロントページの続き

(72)発明者　伊藤　義裕
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　小堀　誠
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　キニ　グレン　マンスフィールド
宮城県仙台市青葉区南吉成六丁目６番地の３　株式会社サイバー・ソリューションズ内

Fターム(参考)　5B085 AC03 AC11 AE00
5B089 GB02 KA17 KB04
5K030 GA15 HB08 HC01 JA10 MB09
MC07 MC08